サイバーセキュリティ通信【R7-10】

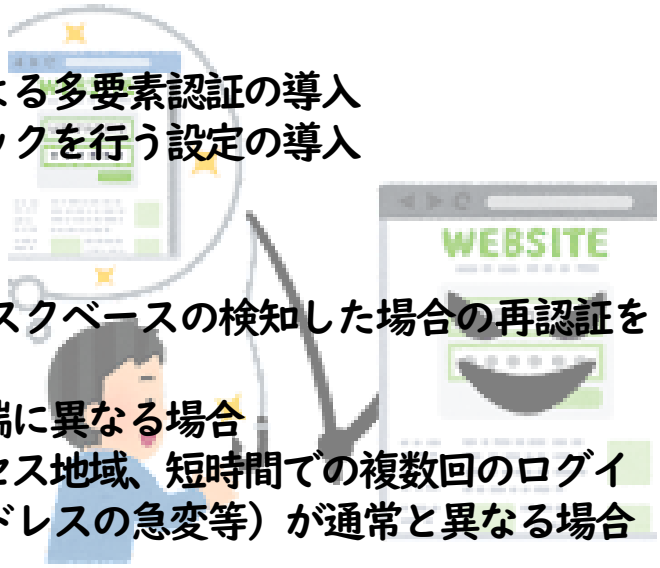
令和7年8月
大分県警察本部生活安全部
サイバー犯罪対策課

不正アクセスによる不正な取引が増加中!!

メール・SMSから誘導されるフィッシング被害防止の対策をお願いします。

Point① 認証の強化

- 生体認証等を用いたパスキーなどによる多要素認証の導入
- 連続ログイン失敗時にアカウントロックを行う設定の導入



Point② 監視・検知能力の強化

- 通常取引と比較して、以下の様なリスクベースの検知した場合の再認証を要求する設定の導入
  （1） 高額出金や取引時間帯が極端に異なる場合
  （2） デバイス環境や挙動（アクセス地域、短時間での複数回のログイン試行、キー入力速度、IPアドレスの急変等）が通常と異なる場合

Point③ なりすまし対策

- 公開ドメイン（サブドメインやメール送信を行わないものも含）について、DMARCの計画導入の検討
- DMARCは、受信者側でなりすましメールの受信拒否を要求するポリシーで運用する

Point④ その他

- ログイン画面・取引画面の録画・スクリーンキャプチャ防止技術の導入
- 顧客端末の脆弱性を自動検知し、脆弱端末からのアクセスを制限・警告を表示する設定の導入

顧客に対する注意喚起を引き続きお願いします。

- 不審なメール・SMSや添付ファイルを開かない
- OS・セキュリティソフトは常に最新状態を保つ、定期的なセキュリティスキャンを実施する

大分県警察
Oita Prefectural Police